Answers to Review Questions
CWSP Guide to Wireless Security

Chapter 1

Review Questions

1. Each of the following is an advantage that wireless local area networks deliver to businesses except
    a. **greater network security**
    b. increased productivity
    c. time savings
    d. financial savings
2. Another name for a wireless local area network is
    a. **Wi-Fi**
    b. Wireless communication system
    c. Radio frequency identification resource
    d. Wireless network adapter system
3. VoWLAN uses a WLAN for
    a. enhanced security transmissions
    b. **voice communications**
    c. roaming between wired segments
    d. segmentation
4. The primary advantage of wireless technology is
    a. low cost
    b. decreased flexibility
    c. **mobility**
    d. bandwidth
5. A _____ has all the equipment needed for an organization to continue running, including office space and furniture, telephone jacks, computer equipment, and a live telecommunications link.
    a. **hot site**
    b. warm site
    c. cold site
    d. distributed remote access location (DRAL)
6. A WLAN can create interference on other wireless devices but cannot itself be interfered with because of its high microwatt power distribution. True or **False**?
7. At the present time no scientific studies have revealed health problems associated with the absorption of low levels of RF energy by the human body. **True** or False?
8. Many organizations have resisted implementing wireless on a broad scale because of the lack of security in wireless. **True** or False?
9. A zero day attack occurs when an attacker discovers and exploits a previously unknown flaw in software. **True** or False?
10. It is not possible for an attacker to use multiple computers in order to launch an attack. True or **False**?

11. Individuals who actively search for wireless signals to pick up, often by just driving down the street, are participating in an activity known as _____. **war driving**
12. An employee who purchases a wireless access point and brings it into the office in order to provide personal wireless access has installed what is known as a(n) _____. **rogue access point**.
13. A(n)_____ is software or hardware that can view the contents of wireless packets. **wireless packet sniffer**

14. _____ is a general term used to describe worms, viruses, spyware, or other types of software that has a malicious intent. **Malware**
15. Almost all _____ have clauses in their contracts that prohibit users from sharing a wireless Internet connection with members outside of the household. **Internet Service Provider (ISP)**
16. Explain how information security can be achieved.

Information security is achieved through a combination of three entities. Information, hardware, software, and communications are protected in three successive layers. The innermost layer consists of the products that provide the necessary security. These products may be as basic as door locks or as complicated as intrusion-detection systems and firewalls. They form the physical security around the data. The next layer is people. Without people implementing and properly using the security products, the data can never be protected. The final layer consists of procedures, which include the plans and policies established by an organization to ensure that people correctly use the products. These three layers interact with each other. The procedures tell the people how to use the products to protect the information. Thus, information security protects the integrity, confidentiality, and availability of information on the devices that sstore, manipulate, and transmit the information through products, people, and procedures.

17. What is the Wi-Fi organization and what does it do?

A consortium of wireless equipment manufacturers and software providers was formed to promote wireless network technology. This group was known as the Wireless Ethernet Compatibility Alliance (WECA). The WECA had three goals: to encourage wireless manufacturers to use the IEEE 802.11 technologies in their wireless networking products; to promote and market these technologies to consumers in the home, in small office home office (SOHO) settings, and in large enterprise businesses and organizations; and to test and certify that wireless products adhere to the IEEE 802.11 standards to ensure product interoperability. In October 2002 the WECA organization changed its name to Wi-Fi (Wireless Fidelity) Alliance, which reflected the name of the certification that it uses (Wi-Fi) to verify that a product follows IEEE standards.

18. What is the role of the Federal Communications Commission in relation to WLANs?

In the United States, the organization that controls and regulates wireless transmissions is the Federal Communications Commission (FCC). The FCC serves as the primary regulatory agency for wireless communications in the United States and its territorial possessions. The FCC is an independent government agency that is directly responsible to Congress, established by the Communications Act of 1934 and charged with regulating interstate and international communications by radio, television, wire, satellite and cable. The FCC is charged with the regulating the radio frequency spectrum.

19. What are the characteristics of an IEEE 802.11b WLAN?

The IEEE 802.11b was added to the original IEEE 802.11 standard, which added two higher speeds (5.5 Mbps and 11 Mbps) to the original 802.11 standard (1 Mbps and 2 Mbps). Like the 802.11 standard, 802.11b also uses the ISM band. The 802.11b standard can support wireless devices that are up to 115 meters (375 feet) apart. However, devices that are that far apart might not be transmitting at 11 Mbps. Radio waves decrease in power over distance. Instead of completely dropping the signal if it falls out of range to transmit at 11 Mbps, the 802.11b standard specifies that the devices should drop their transmission speed to the next lower level (5.5, 2, or 1 Mbps). This allows devices to transmit farther apart but at slower speeds

20. What are the expected features of the IEEE 802.11n standard?

In September of 2004 the IEEE started working on a new standard to significantly increase the bandwidth of today's WLANs. Known as 802.11n or Multiple-Input, Musltiple-Output Enhanced WLAN (MEW), it will set standards for transmissions exceeding 300 Mbps. The 802.11n committee is evaluating over 60 different proposals regarding how to accomplish this. The top speed of the 802.11n standard will be anywhere from 300 Mbps to 600 Mbps, depending on which proposal is approved. The final proposal might not be ratified until the year 2007